Some applications of Kummer and Stickelberger relations

Roland Quême

2006 april 19

Contents

Abstract

Roland Quême
13 avenue du château d'eau
31490 Brax
France
tel : 0561067020
cel : 0684728729
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/
****
V10 - MSC Classification : 11R18; 11R29
****
Let p be an odd prime. Let $\mathbf{F}_p$ be the finite field of p elements with no null part $\mathbf{F}_p^*$. Let $K_p = \mathbb{Q}(\zeta_p)$ be the p-cyclotomic field. Let π be the prime ideal of K_p lying over p. Let v be a primitive root $\mod p$. In the sequel of this paper, for $n \in \mathbb{Z}$ let us note briefly v^n for $v^n \mod p$ with $1 \leq v^n \leq p-1$. Let $\sigma : \zeta_p \rightarrow \zeta_p^v$ be a $\mathbb{Q}$-isomorphism of $K_p/\mathbb{Q}$. Let G_p be the Galois group of $K_p/\mathbb{Q}$. Let $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i}, \quad P(\sigma) \in \mathbb{Z}[G_p]$.

We suppose that p is an irregular prime. Let C_p be the p-class group of K_p. Let Γ be a subgroup of C_p of order p annihilated by $\sigma - \mu$ with $\mu \in \mathbf{F}_p^*$. From Kummer, there exist not principal prime ideals $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ of inertial degree 1 with class $Cl(\mathbf{q}) \in \Gamma$. Let q be the prime number lying above $\mathbf{q}$.

Let n be the smallest natural integer $1 < n \leq p-2$ such that $\mu \equiv v^n \mod p$ for μ defined above. There exist singular numbers A with $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$ and $\pi^n \mid A - a$ where a is a natural number. If A is singular not primary then $\pi^n \parallel A - a$ and if A is singular primary then $\pi^p \mid A - a$. We prove, by an application of Stickelberger relation to the prime ideal $\mathbf{q}$, that now we can *climb* up to the π-adic congruence:

1. $\pi^{2p-1} \mid A^{P(\sigma)}$ if $q \equiv 1 \mod p$.
2. $\pi^{2p-1} \parallel A^{P(\sigma)}$ if $q \equiv 1 \mod p$ and $p^{(q-1)/p} \equiv 1 \mod q$.
3. $\pi^{2p} \mid A^{P(\sigma)}$ if $q \not\equiv 1 \mod p$.

This property of π-adic congruences on singular numbers is at the heart of this paper.

1. As a first example, in section 3 p. 15 this π-adic improvement allows us to give an elementary straightforward proof that the relative p-class group C_p^- verifies the following congruence $\mod p$: with v, m defined above, the congruence

$$(1) \qquad \sum_{i=1}^{p-2} v^{(2m+1)(i-1)} \times \left(\frac{v^{-(i-1)} - v^{-i} \times v}{p}\right) \equiv 0 \mod p,$$

is verified for m taking r^- different values m_i, $\quad i = 1, \dots, r^-$ where r^- is the rank of the relative p-class group C_p^- (result which can also be proved by annihilation of class group of K_p by Stickelberger ideal $\in \mathbb{Z}[G_p]$). A second example is a straightforward proof that if $\frac{p-1}{2}$ is odd then the Bernoulli Number $B_{(p+1)/2} \not\equiv 0 \mod p$.

2. The section 4 p. 18 brings some results on connection between singular primary numbers and the stucture of the p-class group of K_p.
3. In the last section 5 p. 20 we give some explicit congruences derived of Stickelberger for prime ideals $\mathbf{q}$ of inertial degree $f > 1$.

1 Some definitions

In this section we give the definitions and notations on cyclotomic fields, p-class group, singular numbers, primary and not primary, used in this paper.

1. Let p be an odd prime. Let ζ_p be a root of the polynomial equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let K_p be the p-cyclotomic field $K_p = \mathbb{Q}(\zeta_p)$. The ring of integers of K_p is $\mathbb{Z}[\zeta_p]$. Let K_p^+ be the maximal totally real subfield of K_p. The ring of integers of K_p^+ is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ with group of units $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$. Let v be a primitive root $\mod p$ and $\sigma : \zeta_p \to \zeta_p^v$ be a $\mathbb{Q}$-isomorphism of K_p. Let G_p be the Galois group of $K_p/\mathbb{Q}$. Let $\mathbf{F}_p$ be the finite field of cardinal p with no null part $\mathbf{F}_p^*$. Let $\lambda = \zeta_p - 1$. The prime ideal of K_p lying over p is $\pi = \lambda\mathbb{Z}[\zeta_p]$.
2. Suppose that p is irregular. Let C_p be the p-class group of K_p. Let r be the rank of C_p. Let C_p^+ be the p-class group of K_p^+. Then $C_p = C_p^+ \oplus C_p^-$ where C_p^- is the relative p-class group.
3. Let Γ be a subgroup of order p of C_p annihilated by $\sigma - \mu \in \mathbf{F}_p[G_p]$ with $\mu \in \mathbf{F}_p^*$. Then $\mu \equiv v^n \mod p$ with a natural integer n, $\quad 1 < n \leq p-2$.
4. An integer $A \in \mathbb{Z}[\zeta_p]$ is said singular if $A^{1/p} \notin K_p$ and if there exists an ideal $\mathbf{a}$ of $\mathbb{Z}[\zeta_p]$ such that $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$.
   (a) $\underline{\text{If } \Gamma \subset C_p^-:}$ then there exists singular integers A with $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$ where $\mathbf{a}$ is a **not** principal ideal of $\mathbb{Z}[\zeta_p]$ verifying simultaneously

$$
\begin{aligned}
& Cl(\mathbf{a}) \in \Gamma, \\
& \sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K_p, \\
& \mu \equiv v^{2m+1} \mod p, \quad m \in \mathbb{N}, \quad 1 \leq m \leq \frac{p-3}{2}, \\
& \pi^{2m+1} \mid A - a, \quad a \in \mathbb{N}, \quad 1 \leq a \leq p-1,
\end{aligned}
\tag{2}
$$

Moreover, this number A verifies

$$A \times \overline{A} = D^p, \tag{3}$$

for some integer $D \in O_{K_p^+}$.

i. This integer A is singular not primary if $\pi^{2m+1} \parallel A - a$.

ii. This integer A is singular primary if $\pi^p \mid A - a^p$.

(b) <u>If $\Gamma \subset C_p^+$:</u> then there exists singular integers A with $A\mathbb{Z}[\zeta_p] = \mathbf{a}^p$ where $\mathbf{a}$ is a **not** principal ideal of $\mathbb{Z}[\zeta_p]$ verifying simultaneously

$$\begin{aligned} &Cl(\mathbf{a}) \in \Gamma, \\ &\sigma(A) = A^\mu \times \alpha^p, \quad \mu \in \mathbf{F}_p^*, \quad \alpha \in K_p, \\ &\mu \equiv v^{2m} \bmod p, \quad m \in \mathbb{Z}, \quad 1 \leq m \leq \frac{p-3}{2}, \\ &\pi^{2m} \mid A - a, \quad a \in \mathbb{Z}, \quad 1 \leq a \leq p-1, \end{aligned} \tag{4}$$

Moreover, this number A verifies

$$\frac{A}{\overline{A}} = D^p, \tag{5}$$

for some number $D \in K_p^+$.

i. This integer A is singular not primary if $\pi^{2m} \parallel A - a$.

ii. This number A is singular primary if $\pi^p \mid A - a^p$.

2 On Kummer and Stickelberger relation

1. Here we fix a notation for the sequel. Let v be a primitive root $\bmod p$. For every integer $k \in \mathbb{Z}$ then v^k is understood $\bmod p$ so $1 \leq v^k \leq p-1$. If $k < 0$ it is to be understood as $v^k v^{-k} \equiv 1 \bmod p$.

2. Let $q \neq p$ be an odd prime. Let ζ_q be a root of the minimal polynomial equation $X^{q-1} + X^{q-2} + \cdots + X + 1 = 0$. Let $K_q = \mathbb{Q}(\zeta_q)$ be the q-cyclotomic field. The ring of integers of K_q is $\mathbb{Z}[\zeta_q]$. Here we fix a notation for the sequel. Let u be a primitive root $\bmod q$. For every integer $k \in \mathbb{Z}$ then u^k is understood $\bmod q$ so $1 \leq u^k \leq q-1$. If $k < 0$ it is to be understood as $u^k u^{-k} \equiv 1 \bmod q$. Let $K_{pq} = \mathbb{Q}(\zeta_p, \zeta_q)$. Then K_{pq} is the compositum $K_p K_q$. The ring of integers of K_{pq} is $\mathbb{Z}[\zeta_{pq}]$.

3. Let $\mathbf{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over the prime q. Let $m = N_{K_p/\mathbb{Q}}(\mathbf{q}) = q^f$ where f is the smallest integer such that $q^f \equiv 1 \bmod p$. If $\psi(\alpha) = a$ is the image

of $\alpha \in \mathbb{Z}[\zeta_p]$ under the natural map $\psi : \mathbb{Z}[\zeta_p] \to \mathbb{Z}[\zeta_p]/\mathbf{q}$, then for $\psi(\alpha) = a \not\equiv 0$ define a character $\chi_{\mathbf{q}}^{(p)}$ on $\mathbf{F}_m = \mathbb{Z}[\zeta_p]/\mathbf{q}$ by

$$\chi_{\mathbf{q}}^{(p)}(a) = \{\frac{\alpha}{\mathbf{q}}\}_p^{-1} = \overline{\{\frac{\alpha}{\mathbf{q}}\}}_p, \tag{6}$$

where $\{\frac{\alpha}{\mathbf{q}}\} = \zeta_p^c$ for some natural integer c, is the p^{th} power residue character mod $\mathbf{q}$. We define

$$g(\mathbf{q}) = \sum_{x \in \mathbf{F}_m} (\chi_{\mathbf{q}}^{(p)}(x) \times \zeta_q^{Tr_{\mathbf{F}_m/\mathbf{F}_q}(x)}) \in \mathbb{Z}[\zeta_{pq}], \tag{7}$$

and $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p$. It follows that $\mathbf{G}(\mathbf{q}) \in \mathbb{Z}[\zeta_{pq}]$. Moreover $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p \in \mathbb{Z}[\zeta_p]$, see for instance Mollin [3] prop. 5.88 (c) p. 308 or Ireland-Rosen [1] prop. 14.3.1 (c) p. 208.

The Stickelberger's relation is classically:

Theorem 2.1. *In $\mathbb{Z}[\zeta_p]$ we have the ideal decomposition*

$$\mathbf{G}(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^S, \tag{8}$$

with $S = \sum_{t=1}^{p-1} t \times \varpi_t^{-1}$ where $\varpi_t \in Gal(K_p/\mathbb{Q})$ is given by $\varpi_t : \zeta_p \to \zeta_p^t$.

See for instance Mollin [3] thm. 5.109 p. 315 and Ireland-Rosen [1] thm. 2. p.209.

2.1 On the structure of $\mathbf{G}(\mathbf{q})$.

In this subsection we are studying carefully the structure of $g(\mathbf{q})$ and $\mathbf{G}(\mathbf{q})$.

Lemma 2.2. *If $q \not\equiv 1$ mod p then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.*

Proof.

1. Let u be a primitive root mod q. Let $\tau : \zeta_q \to \zeta_q^u$ be a $\mathbb{Q}$-isomorphism generating $Gal(K_q/\mathbb{Q})$. The isomorphism τ is extended to a K_p-isomorphism of K_{pq} by $\tau : \zeta_q \to \zeta_q^u, \quad \zeta_p \to \zeta_p$. Then $g(\mathbf{q})^p = \mathbf{G}(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and so

$$\tau(g(\mathbf{q}))^p = g(\mathbf{q})^p,$$

and it follows that there exists a natural integer ρ with $\rho < p$ such that

$$\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q}).$$

Then $N_{K_{pq}/K_p}(\tau(g(\mathbf{q}))) = \zeta_p^{(q-1)\rho} \times N_{K_{pq}/K_p}(g(\mathbf{q}))$ and so $\zeta_p^{\rho(q-1)} = 1$.

2. If $q \not\equiv 1 \bmod p$, it implies that $\zeta_p^\rho = 1$ and so that $\tau(g(\mathbf{q})) = g(\mathbf{q})$ and thus that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.

$\square$

Let us note in the sequel $g(\mathbf{q}) = \sum_{i=0}^{q-2} g_i \times \zeta_q^i$ with $g_i \in \mathbb{Z}[\zeta_p]$.

Lemma 2.3. *If $q \equiv 1 \bmod p$ then $g_0 = 0$.*

Proof. Suppose that $g_0 \neq 0$ and search for a contradiction: we start of

$$\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q}).$$

We have $g(\mathbf{q}) = \sum_{i=0}^{q-2} g_i \times \zeta_q^i$ and so $\tau(g(\mathbf{q})) = \sum_{i=0}^{q-2} g_i \times \zeta_q^{iu}$, therefore

$$\sum_{i=0}^{q-2} (\zeta_p^\rho g_i) \times \zeta_q^i = \sum_{i=0}^{q-2} g_i \times \zeta_q^{iu},$$

thus $g_0 = \zeta_p^\rho \times g_0$ and so $\zeta_p^\rho = 1$ which implies that $\tau(g(\mathbf{q})) = g(\mathbf{q})$ and so $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$. Then $\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p$ and so Stickelberger relation leads to $g(\mathbf{q})^p \mathbb{Z}[\zeta_p] = \mathbf{q}^S$ where $S = \sum_{t=1}^{p-1} t \times \varpi_t^{-1}$. Therefore $\varpi_1^{-1}(\mathbf{q}) \parallel \mathbf{q}^S$ because q splits totally in $K_p/\mathbb{Q}$ and $\varpi_t^{-1}(\mathbf{q}) \neq \varpi_{t'}^{-1}(\mathbf{q})$ for $t \neq t'$. This case is not possible because the first member $g(\mathbf{q})^p$ is a p-power. $\square$

Here we give an elementary computation of $g(\mathbf{q})$ not involving directly the Gauss Sums.

Lemma 2.4. *If $q \equiv 1 \bmod p$ then*

$$\begin{aligned} &\mathbf{G}(\mathbf{q}) = g(\mathbf{q})^p, \\ &g(\mathbf{q}) = \zeta_q + \zeta_p^\rho \zeta_q^{u^{-1}} + \zeta_p^{2\rho} \zeta_q^{u^{-2}} + \dots \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-2)}}, \\ &g(\mathbf{q})^p \mathbb{Z}[\zeta_p] = \mathbf{q}^S, \end{aligned} \tag{9}$$

for some natural number ρ, $\quad 1 < \rho \leq p-1$.

Proof.

1. We start of $\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q})$ and so

$$\sum_{i=1}^{q-2} g_i \zeta_q^{ui} = \zeta_p^\rho \times \sum_{i=1}^{q-2} g_i \zeta_q^i, \tag{10}$$

which implies that $g_i = g_1 \zeta_p^\rho$ for $u \times i \equiv 1 \bmod q$ and so $g_{u^{-1}} = g_1 \zeta_p^\rho$ (where u^{-1} is to be understood by $u^{-1} \bmod q$, so $1 \leq u^{-1} \leq q-1$).

2. Then $\tau^2(g(\mathbf{q})) = \tau(\zeta_p^\rho g(\mathbf{q})) = \zeta_p^{2\rho} g(\mathbf{q})$. Then

$$\sum_{i=1}^{q-2} g_i \zeta_q^{u^2 i} = \zeta_p^{2\rho} \times (\sum_{i=1}^{q-2} g_i \zeta_q^i),$$

   which implies that $g_i = g_1 \zeta_p^{2\rho}$ for $u^2 \times i \equiv 1 \bmod q$ and so $g_{u^{-2}} = g_1 \zeta_p^{2\rho}$.

3. We continue up to $\tau^{(q-2)\rho}(g(\mathbf{q})) = \tau^{q-3}(\zeta_p^\rho g(\mathbf{q})) = \cdots = \zeta_p^{(q-2)\rho} g(\mathbf{q})$. Then

$$\sum_{i=1}^{q-2} g_i \zeta_q^{u^{q-2} i} = \zeta_p^{(q-2)\rho} \times (\sum_{i=1}^{q-2} g_i \zeta_q^i),$$

   which implies that $g_i = g_1 \zeta_p^{(q-2)\rho}$ for $u^{q-2} \times i \equiv 1 \bmod q$ and so $g_{u^{-(q-2)}} = g_1 \zeta_p^{(q-2)\rho}$.

4. Observe that u is a primitive root $\bmod q$ and so u^{-1} is a primitive root $\bmod q$. Then it follows that $g(\mathbf{q}) = g_1 \times (\zeta_q + \zeta_p^\rho \zeta_q^{u^{-1}} + \zeta_p^{2\rho} \zeta_q^{u^{-2}} + \ldots \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-2)}})$. Let $U = \zeta_q + \zeta_p^\rho \zeta_q^{u^{-1}} + \zeta_p^{2\rho} \zeta_q^{u^{-2}} + \ldots \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-2)}}$.

5. We prove now that $g_1 \in \mathbb{Z}[\zeta_p]^*$. From Stickelberger relation $g_1^p \times U^p = \mathbf{q}^S$. From $S = \sum_{i=1}^{p-1} \varpi_t^{-1} \times t$ it follows that $\varpi_t^{-1}(\mathbf{q})^t \parallel \mathbf{q}^S$ and so that $g_1 \not\equiv 0 \bmod \varpi_t^{-1}(\mathbf{q})$ because g_1^p is a p-power, which implies that $g_1 \in \mathbb{Z}[\zeta_p]^*$. Let us consider the relation(7). Let $x = 1 \in \mathbf{F}_q$, then $Tr_{\mathbf{F}_q/\mathbf{F}_q}(x) = 1$ and $\chi_{\mathbf{q}}^{(p)}(1) = 1^{(q-1)/p} \bmod \mathbf{q} = 1$ and thus the coefficient of ζ_q is 1 and so $g_1 = 1$.

6. From Stickelberger, $g(\mathbf{q})^p \mathbb{Z}[\zeta_p] = \mathbf{q}^S$, which achieves the proof.

□

Remark: From

$$\begin{aligned} & g(\mathbf{q}) = \zeta_q + \zeta_p^\rho \zeta_q^{u^{-1}} + \zeta_p^{2\rho} \zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-2)}}, \\ & \Rightarrow \tau(g(\mathbf{q})) = \zeta_q^u + \zeta_p^\rho \zeta_q + \zeta_p^{2\rho} \zeta_q^{u^{-1}} + \cdots + \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-3)}}, \\ & \Rightarrow \zeta^\rho \times g(\mathbf{q}) = \zeta^\rho \zeta_q + \zeta_p^{2\rho} \zeta_q^{u^{-1}} + \zeta_p^{3\rho} \zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-1)\rho} \zeta_q^{u^{-(q-2)}} \end{aligned} \tag{11}$$

and we can verify directly that $\tau(g(\mathbf{q})) = \zeta_p^\rho \times g(\mathbf{q})$ for this expression of $g(\mathbf{q})$, observing that $q - 1 \equiv 0 \bmod p$.

Lemma 2.5. *Let $S = \sum_{t=1}^{p-1} \varpi_t^{-1} \times t$ where ϖ_t is the $\mathbb{Q}$-isomorphism given by $\varpi_t : \zeta_p \to \zeta_p^t$ of K_p. Let v be a primitive root $\bmod p$. Let σ be the $\mathbb{Q}$-isomorphism of K_p given by $\zeta_p \to \zeta_p^v$. Let $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i} \in \mathbb{Z}[G_p]$. Then $S = P(\sigma)$.*

Proof. Let us consider one term $\varpi_t^{-1} \times t$. Then $v^{-1} = v^{p-2}$ is a primitive root $\bmod p$ because $p-2$ and $p-1$ are coprime and so there exists one and one i such that $t = v^{-i}$. Then $\varpi_{v^{-i}} : \zeta_p \to \zeta_p^{v^{-i}}$ and so $\varpi_{v^{-i}}^{-1} : \zeta_p \to \zeta_p^{v^i}$ and so $\varpi_{v^{-i}}^{-1} = \sigma^i$ (observe that $\sigma^{p-1} \times v^{-(p-1)} = 1$), which achieves the proof. □

Remark : The previous lemma is a verification of the consistency of results in Ribenboim [5] p. 118, of Mollin [3] p. 315 and of Ireland-Rosen p. 209 with our computation. In the sequel we use Ribenboim notation more adequate for the factorization in $\mathbf{F}_p[G]$. In that case the Stickelberger's relation is connected with the Kummer's relation on Jacobi resolvents, see for instance Ribenboim, [5] (2A) b. p. 118 and (2C) relation (2.6) p. 119.

Lemma 2.6. *If $q \equiv 1 \bmod p$ then*

1. *$g(\mathbf{q})$ defined in relation (9) is a Jacobi resolvent: $g(\mathbf{q}) = <\zeta_p^\rho, \zeta_q>$.*
2. *$\rho = -v$.*

Proof.

1. Apply formula of Ribenboim [5] (2.2) p. 118 with $p = p, q = q, \zeta = \zeta_p, \quad \rho = \zeta_q, \quad n = \rho, \quad u = i, \quad m = 1$ and $h = u^{-1}$ (where the left members notations $p, q, \zeta, \rho, n, u, m$ and h are the Ribenboim notations).
2. We start of $<\zeta_p^\rho, \zeta_q> = g(\mathbf{q})$. Then v is a primitive root $\bmod p$, so there exists a natural integer l such that $\rho \equiv v^l \bmod p$. By conjugation σ^{-l} we get $<\zeta_p, \zeta_q> = g(\mathbf{q})^{\sigma^{-l}}$. Raising to p-power $<\zeta_p, \zeta_q>^p = g(\mathbf{q})^{p\sigma^{-l}}$. From lemma 2.5 and Stickelberger relation $<\zeta_p, \zeta_q>^p \mathbb{Z}[\zeta_p] = \mathbf{q}^{P(\sigma)\sigma^{-l}}$. From Kummer's relation (2.6) p. 119 in Ribenboim [5], we get $<\zeta_p, \zeta_q>^p \mathbb{Z}[\zeta_p] = \mathbf{q}^{P_1(\sigma)}$ with $P_1(\sigma) = \sum_{j=0}^{p-2} \sigma^j v^{(p-1)/2-j}$. Therefore $\sum_{i=0}^{p-2} \sigma^{i-l} v^{-i} = \sum_{j=0}^{p-2} \sigma^j v^{(p-1)/2-j}$. Then $i - l \equiv j \bmod p$ and $-i \equiv \frac{p-1}{2} - j \bmod p$ (or $i \equiv j - \frac{p-1}{2} \bmod p$) imply that $j - \frac{p-1}{2} - l \equiv j \bmod p$, so $l + \frac{p-1}{2} \equiv 0 \bmod p$, so $l \equiv -\frac{p-1}{2} \bmod p$, and $l \equiv \frac{p+1}{2} \bmod p$, thus $\rho \equiv v^{(p+1)/2} \bmod p$ and finally $\rho = -v$.

□

Remark : The previous lemma allows to verify the consistency of our computation with Jacobi resultents used in Kummer (see Ribenboim p. 118-119).

Lemma 2.7. *If $\mathbf{q} \equiv 1 \bmod p$ then $g(\mathbf{q}) \equiv -1 \bmod \pi$.*

Proof. From $g(\mathbf{q}) = \zeta_q + \zeta_p^\rho \zeta_q^{u^{-1}} + \zeta_p^{2\rho} \zeta_q^{u^{-2}} + \cdots + \zeta_p^{(q-2)\rho} \zeta_q^{u^{-(q-2)}}$, we see that $g(\mathbf{q}) \equiv \zeta_q + \zeta_q^{u^{-1}} + \zeta_q^{u^{-2}} + \cdots + \zeta_q^{u^{-(q-2)}} \bmod \pi$. From u^{-1} primitive root $\bmod p$ it follows that $1 + \zeta_q + \zeta_q^{u^{-1}} + \zeta_q^{u^{-2}} + \cdots + \zeta_q^{u^{-(q-2)}} = 0$, which leads to the result. □

It is possible to improve the previous result to:

Lemma 2.8. *Suppose that $q \equiv 1$ mod p. If $p^{(q-1)/p} \not\equiv 1$ mod q then $\pi^p \parallel g(\mathbf{q})^p + 1$.*

Proof.

1. We start of $g(\mathbf{q}) = \zeta_q + \zeta_p^{\rho}\zeta_q^{u^{-1}} + \zeta_p^{2\rho}\zeta_q^{u^{-2}} + \dots \zeta_p^{(q-2)\rho}\zeta_q^{u^{-(q-2)}}$, so

   $$g(\mathbf{q}) = \zeta_q + ((\zeta_p^{\rho}-1)+1)\zeta_q^{u^{-1}} + ((\zeta_p^{2\rho}-1)+1)\zeta_q^{u^{-2}}, + \dots ((\zeta_p^{(q-2)\rho}-1)+1)\zeta_q^{u^{-(q-2)}}$$

   also

   $$g(\mathbf{q}) = -1 + (\zeta_p^{\rho}-1)\zeta_q^{u^{-1}} + (\zeta_p^{2\rho}-1)\zeta_q^{u^{-2}} + \dots + (\zeta_p^{(q-2)\rho}-1)\zeta_q^{u^{-(q-2)}}.$$

   Then $\zeta_p^{i\rho} \equiv 1 + i\rho\lambda \bmod \pi^2$, so

   $$g(\mathbf{q}) \equiv -1 + \lambda \times (\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \dots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \bmod \lambda^2.$$

   Then $g(\mathbf{q}) = -1 + \lambda U + \lambda^2 V$ with $U = \rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \dots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}$ and $U, V \in \mathbb{Z}[\zeta_{pq}]$.

2. Suppose that $\pi^{p+1} \mid g(\mathbf{q})^p + 1$ and search for a contradiction: then, from $g(\mathbf{q})^p = (-1 + \lambda U + \lambda^2 V)^p$, it follows that $p\lambda U + \lambda^p U^p \equiv 0 \bmod \pi^{p+1}$ and so $U^p - U \equiv 0 \bmod \pi$ because $p\lambda + \lambda^p \equiv 0 \bmod \pi^{p+1}$. Therefore

   $$(\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \dots + (q-2)\rho)\zeta_q^{u^{-(q-2)}})^p -$$
   $$(\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \dots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \equiv 0 \bmod \lambda,$$

   and so

   $$(\rho\zeta_q^{pu^{-1}} + 2\rho\zeta_q^{pu^{-2}} + \dots + (q-2)\rho)\zeta_q^{pu^{-(q-2)}})$$
   $$- (\rho\zeta_q^{u^{-1}} + 2\rho\zeta_q^{u^{-2}} + \dots + (q-2)\rho)\zeta_q^{u^{-(q-2)}}) \equiv 0 \bmod \lambda.$$

3. For any natural j with $1 \leq j \leq q-2$, there must exist a natural j' with $1 \leq j' \leq q-2$ such that simultaneously:

   $$pu^{-j'} \equiv u^{-j} \bmod q \Rightarrow p \equiv u^{j'-j} \bmod q,$$
   $$\Rightarrow \rho j' \equiv \rho j \bmod \pi \Rightarrow j' - j \equiv 0 \bmod p.$$

   Therefore $p \equiv u^{p \times \{(j'-j)/p\}} \bmod q$ and so $p^{(q-1)/p} \equiv u^{p \times (q-1)/p) \times \{(j'-j)/p\}} \bmod q$ thus $p^{(q-1)/p} \equiv 1 \bmod q$, contradiction.

∎

2.2 A study of polynomial $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i v^{-i}$ of $\mathbb{Z}[G_p]$.

Recall that $P(\sigma) \in \mathbb{Z}[G_p]$ has been defined by $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i v^{-i}$.

Lemma 2.9.

$$P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v^{-i} = v^{-(p-2)} \times \{ \prod_{k=0,\ k\neq 1}^{p-2} (\sigma - v^k)\} + p \times R(\sigma), \tag{12}$$

where $R(\sigma) \in \mathbb{Z}[G_p]$ *with* $deg(R(\sigma)) < p-2$.

Proof. Let us consider the polynomial $R_0(\sigma) = P(\sigma) - v^{-(p-2)} \times \{\prod_{k=0,\ k\neq 1}^{p-2} (\sigma - v^k)\}$ in $\mathbf{F}_p[G_p]$. Then $R_0(\sigma)$ is of degree smaller than $p-2$ and the two polynomials $\sum_{i=0}^{p-2} \sigma^i v^{-i}$ and $\prod_{k=0,\ k\neq 1}^{p-2}(\sigma - v^k)$ take a null value in $\mathbf{F}_p[G_p]$ when σ takes the $p-2$ different values $\sigma = v^k$ for $k = 0, \dots, p-2, \quad k \neq 1$. Then $R_0(\sigma) = 0$ in $\mathbf{F}_p[G_p]$ which leads to the result in $\mathbb{Z}[G_p]$. □

Let us note in the sequel

$$T(\sigma) = v^{-(p-2)} \times \prod_{k=0,\ k\neq 1}^{p-2} (\sigma - v^k). \tag{13}$$

Lemma 2.10.

$$P(\sigma) \times (\sigma - v) = T(\sigma) \times (\sigma - v) + pR(\sigma) \times (\sigma - v) = p \times Q(\sigma), \tag{14}$$

where $Q(\sigma) = \sum_{i=1}^{p-2} \delta_i \times \sigma^i \in \mathbb{Z}[G_p]$ *is given by*

$$\begin{aligned}
\delta_{p-2} &= \frac{v^{-(p-3)} - v^{-(p-2)}v}{p}, \\
\delta_{p-3} &= \frac{v^{-(p-4)} - v^{-(p-3)}v}{p}, \\
&\vdots \\
\delta_i &= \frac{v^{-(i-1)} - v^{-i}v}{p}, \\
&\vdots \\
\delta_1 &= \frac{1 - v^{-1}v}{p},
\end{aligned} \tag{15}$$

with $-p < \delta_i \leq 0$.

Proof. We start of the relation in $\mathbb{Z}[G_p]$

$$P(\sigma)\times(\sigma-v)=v^{-(p-2)}\times\prod_{k=0}^{p-2}(\sigma-v^k)+p\times R(\sigma)\times(\sigma-v)=p\times Q(\sigma),$$

with $Q(\sigma)\in\mathbb{Z}[G_p]$ because $\prod_{k=0}^{p-2}(\sigma-v^k)=0$ in $\mathbf{F}_p[G_p]$ and so $\prod_{k=0}^{p-2}(\sigma-v^k)=p\times R_1(\sigma)$ in $\mathbb{Z}[G_p]$. Then we identify in $\mathbb{Z}[G_p]$ the coefficients in the relation

$$\begin{aligned}&(v^{-(p-2)}\sigma^{p-2}+v^{-(p-3)}\sigma^{p-3}+\cdots+v^{-1}\sigma+1)\times(\sigma-v)=\\&p\times(\delta_{p-2}\sigma^{p-2}+\delta_{p-3}\sigma^{p-3}+\cdots+\delta_1\sigma+\delta_0),\end{aligned}$$

where $\sigma^{p-1}=1$. $\square$

Remark:

1. Observe that, with our notations, $\delta_i\in\mathbb{Z},\quad i=1,\dots,p-2$, but generally $\delta_i\not\equiv 0 \bmod p$.
2. We see also that $-p<\delta_i\leq 0$. Observe also that $\delta_0=\frac{v^{-(p-2)}-v}{p}=0$.

Lemma 2.11. *The polynomial $Q(\sigma)$ verifies*

$$Q(\sigma)=\{(1-\sigma)(\sum_{i=0}^{(p-3)/2}\delta_i\times\sigma^i)+(1-v)\sigma^{(p-1)/2}\}\times(\sum_{i=0}^{(p-3)/2}\sigma^i). \tag{16}$$

Proof. We start of $\delta_i=\frac{v^{-(i-1)}-v^{-i}v}{p}$. Then

$$\delta_{i+(p-1)/2}=\frac{v^{-(i+(p-1)/2-1)}-v^{-(i+(p-1)/2)}}{p}=\frac{p-v^{-(i-1)}-(p-v^{-i})v}{p}=1-v-\delta_i.$$

Then

$$\begin{aligned}Q(\sigma)&=\sum_{i=0}^{(p-3)/2}(\delta_i\times(\sigma^i-\sigma^{i+(p-1)/2}+(1-v)\sigma^{i+(p-1)/2})\\&=(\sum_{i=0}^{(p-3)/2}\delta_i\times\sigma^i)\times(1-\sigma^{(p-1)/2)})+(1-v)\times\sigma^{(p-1)/2}\times(\sum_{i=0}^{(p-3)/2}\sigma^i),\end{aligned}$$

which leads to the result. $\square$

2.3 π-adic congruences on the singular integers A

From now we suppose that the prime ideal $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ has a class $Cl(\mathbf{q}) \in \Gamma$ where Γ is a subgroup of order p of C_p previously defined, with a singular integer A given by $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$.

In an other part, we know that the group of ideal classes of the cyclotomic field is generated by the ideal classes of prime ideals of degree 1, see for instance Ribenboim, [5] (3A) p. 119.

Lemma 2.12.
$(\frac{g(\mathbf{q}}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^{P(\sigma)}$.

Proof. We start of $\mathbf{G}(\mathbf{q})\mathbb{Z}[\zeta_p] = g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$. Raising to p-power we get $g(\mathbf{q})^{p^2}\mathbb{Z}[\zeta_p] = \mathbf{q}^{pS}$. But $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$, so

$$g(\mathbf{q})^{p^2}\mathbb{Z}[\zeta_p] = A^S\mathbb{Z}[\zeta_p], \tag{17}$$

so

$$g(\mathbf{q})^{p^2} \times \zeta_p^w \times \eta = A^S, \quad \eta \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*, \tag{18}$$

where w is a natural number. Therefore, by complex conjugation, we get $\overline{g(\mathbf{q})}^{p^2} \times \zeta_p^{-w} \times \eta = \overline{A}^S$. Then $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} \times \zeta_p^{2w} = (\frac{A}{\overline{A}})^S$. From $A \equiv a \mod \pi^{2m+1}$ with a natural integer, we get $\frac{A}{\overline{A}} \equiv 1 \mod \pi^{2m+1}$ and so $w = 0$. Then $(\frac{g(\mathbf{q})}{\overline{g(\mathbf{q})}})^{p^2} = (\frac{A}{\overline{A}})^S$. $\square$

Remark: Observe that this lemma is true if either $q \equiv 1 \mod p$ or $q \not\equiv 1 \mod p$.

Theorem 2.13.

1. $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$.
2. $g(\mathbf{q})^{p(\sigma-1)(\sigma-v)} = \pm(\frac{\overline{A}}{A})^{Q_1(\sigma)}$ *where*

$$Q_1(\sigma) = (1-\sigma) \times (\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) + (1-v) \times \sigma^{(p-1)/2}.$$

Proof.

1. We start of $g(\mathbf{q})^{p^2} \times \eta = A^{P(\sigma)}$ proved. Then $g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = A^{P(\sigma)(\sigma-1)(\sigma-v)}$. From lemma 2.11, we get

$$P(\sigma) \times (\sigma - v) \times (\sigma - 1) = p \times Q_1(\sigma) \times (\sigma^{(p-1)/2} - 1),$$

where

$$Q_1(\sigma) = (1-\sigma)\times(\sum_{i=0}^{(p-3)/2} \delta_i \times \sigma^i) + (1-v)\times\sigma^{(p-1)/2}.$$

Therefore

$$g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = (\frac{\overline{A}}{A})^{pQ_1(\sigma)}, \tag{19}$$

and by conjugation

$$\overline{g(\mathbf{q})}^{p^2(\sigma-1)(\sigma-v)} \times \eta^{(\sigma-1)(\sigma-v)} = (\frac{A}{\overline{A}})^{pQ_1(\sigma)}.$$

Multiplying these two relations we get, observing that $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q^f$,

$$q^{fp^2(\sigma-1)(\sigma-v)} \times \eta^{2(\sigma-1)(\sigma-v)} = 1,$$

also

$$\eta^{2(\sigma-1)(\sigma-v)} = 1,$$

and thus $\eta = \pm 1$ because $\eta \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$, which with relation (19) get $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ achieves the proof of the first part.

2. From relation (19) we get

$$g(\mathbf{q})^{p^2(\sigma-1)(\sigma-v)} = \pm(\frac{\overline{A}}{A})^{pQ_1(\sigma)}, \tag{20}$$

so

$$g(\mathbf{q})^{p(\sigma-1)(\sigma-v)} = \pm\zeta_p^w \times (\frac{\overline{A}}{A})^{Q_1(\sigma)}, \tag{21}$$

where w is a natural number. But $g(\mathbf{q})^{\sigma-v} \in K_p$ and so $g(\mathbf{q})^{p(\sigma-v)(\sigma-1)} \in (K_p)^p$, see for instance Ribenboim [5] (2A) b. p. 118. and $(\frac{\overline{A}}{A})^{Q_1(\sigma)} \in (K_p)^p$ because $\sigma - \mu \mid Q_1(\sigma)$ in $\mathbf{F}_p[G_p]$ imply that $w = 0$, which achieves the proof of the second part.

$\square$

Remarks

1. Observe that this theorem is true either $q \equiv 1 \bmod p$ or $q \not\equiv 1 \bmod p$.
2. $g(\mathbf{q}) \equiv -1 \bmod \pi$ implies that $g(\mathbf{q})^{p^2} \equiv -1 \bmod \pi$. Observe that if $A \equiv a \bmod \pi$ with a natural number then $A^{P(\sigma)} \equiv a^{1+v^{-1}+\dots+v^{-(p-2)}} = a^{p(p-1)/2} \bmod \pi \equiv \pm 1 \bmod \pi$ consistent with previous result.

Lemma 2.14. *Let $q \neq p$ be an odd prime. Let f be the smallest integer such that $q^f \equiv 1 \bmod p$. If f is even then $g(\mathbf{q}) = \pm\zeta_p^w q^{f/2}$ for w a natural number.*

Proof.

1. Let $\mathbf{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. From f even we get $\mathbf{q} = \overline{\mathbf{q}}$. As in first section there exists singular numbers A such that $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$.
2. From $\mathbf{q} = \overline{\mathbf{q}}$ we can choose $A \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and so $A = \overline{A}$.
3. we have $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$. From lemma 2.2 p. 5, we know that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.
4. By complex conjugation $\overline{g(\mathbf{q})^{p^2}} = \pm A^{P(\sigma)}$. Then $g(\mathbf{q})^{p^2} = \overline{g(\mathbf{q})}^{p^2}$.
5. Therefore $g(\mathbf{q})^p = \zeta_p^{w_2} \times \overline{g(\mathbf{q})}^p$ with w_2 natural number. As $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ this implies that $w_2 = 0$ and so $g(\mathbf{q})^p = \overline{g(\mathbf{q})}^p$. Therefore $g(\mathbf{q}) = \zeta_p^{w_3} \times \overline{g(\mathbf{q})}$ with w_3 natural number. But $g(\mathbf{q}) \times \overline{g(\mathbf{q})} = q^f$ results of properties of power residue Gauss sums, see for instance Mollin prop 5.88 (b) p. 308. Therefore $g(\mathbf{q})^2 = \zeta_p^{w_3} \times q^f$ and so $(g(\mathbf{q}) \times \zeta_p^{-w_3/2})^2 = q^f$ and thus $g(\mathbf{q}) \times \zeta_p^{-w_3/2} = \pm q^{f/2}$ wich achieves the proof.

□

Theorem 2.15.

1. *If $q \equiv 1 \bmod p$ then $A^{P(\sigma)} \equiv \delta \bmod \pi^{2p-1}$ with $\delta \in \{-1, 1\}$.*
2. *If and only if $q \equiv 1 \bmod p$ and $p^{(q-1)/p} \equiv 1 \bmod q$ then $\pi^{2p-1} \parallel A^{P(\sigma)} - \delta$ with $\delta \in \{-1, 1\}$.*
3. *If $q \not\equiv 1 \bmod p$ then $A^{P(\sigma)} \equiv \delta \bmod \pi^{2p}$ with $\delta \in \{-1, 1\}$.*

Proof.

1. From lemma 2.7, we get $\pi^p \mid g(\mathbf{q})^p + 1$ and so $\pi^{2p-1} \mid g(\mathbf{q})^{p^2} + 1$. Then apply theorem 2.13.
2. Applying lemma 2.8 we get $\pi^p \parallel g(\mathbf{q})^p + 1$ and so $\pi^{2p-1} \parallel g(\mathbf{q})^{p^2} + 1$. Then apply theorem 2.13.
3. From lemma 2.2, then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and so $\pi^{p+1} \mid g(\mathbf{q})^p + 1$ and also $\pi^{2p} \mid g(\mathbf{q})^{p^2} + 1$.

□

Remark: If $C \in \mathbb{Z}[\zeta_p]$ is any semi-primary number with $C \equiv c \bmod \pi^2$ with c natural number we can only assert in general that $C^{P(\sigma)} \equiv \pm 1 \bmod \pi^{p-1}$. For the singular numbers A considered here we assert more: $A^{P(\sigma)} \equiv \pm 1 \bmod \pi^{2p-1}$. We shall use this π-adic improvement in the sequel.

3 Explicit polynomial congruences mod p connected to the p-class group

We deal of explicit polynomial congruences connected to the p-class group when p not divides the class number h^+ of K_p^+.

1. We know that the relative p-class group $C_p^- = \oplus_{k=1}^{r^-}\Gamma_k$ where Γ_k are groups of order p annihilated by $\sigma-\mu_k$, $\mu_k \equiv v^{2m_k+1} \bmod p$, $1 \le m_k \le \frac{p-3}{2}$. Let us consider the singular numbers A_k, $k=1,\dots,r^-$, with $\pi^{2m_k+1} \mid A_k-\alpha_k$ with α_k natural number defined in lemmas 2.9 and 2.10. From Kummer, the group of ideal classes of K_p is generated by the classes of prime ideals of degree 1 (see for instance Ribenboim [5] (3A) p. 119).
2. In this section we shall explicit a connection between the polynomial $Q(\sigma) \in \mathbb{Z}[G_p]$ and the structure of the relative p-class group C_p^- of K_p.
3. As another example we shall give an elementary proof in a straightforward way that if $\frac{p-1}{2}$ is odd then the Bernoulli Number $B_{(p+1)/2} \not\equiv 0 \bmod p$.

Theorem 3.1. *Let p be an odd prime. Let v be a primitive root mod p. For $k=1,\dots,r^-$ rank of the p-class group of K_p then*

$$Q(v^{2m_k+1}) = \sum_{i=1}^{p-2} v^{(2m_k+1)\times i} \times (\frac{v^{-(i-1)}-v^{-i}\times v}{p}) \equiv 0 \ mod\ p, \tag{22}$$

(or an other formulation $\prod_{k=1}^{r^-}(\sigma - v^{2m_k+1})$ divides $Q(\sigma)$ in $\mathbf{F}_p[G_p]$).

Proof.

1. Let us fix A for one the singular numbers A_k with $\pi^{2m+1} \parallel A-\alpha$ with α natural number equivalent to $\pi^{2m+1} \parallel (\frac{A}{\overline{A}}-1)$, equivalent to
$$\frac{A}{\overline{A}} = 1+\lambda^{2m+1}\times a, \quad a \in K_p, \quad v_\pi(a)=0.$$
Then raising to p-power we get $(\frac{A}{\overline{A}})^p = (1+\lambda^{2m+1}\times a)^p \equiv 1+p\lambda^{2m+1}a \bmod \pi^{p-1+2m+2}$ and so $\pi^{p-1+2m+1} \parallel (\frac{A}{\overline{A}})^p - 1$.
2. From theorem 2.15 we get
$$(\frac{A}{\overline{A}})^{P(\sigma)\times(\sigma-v)} = (\frac{A}{\overline{A}})^{pQ(\sigma)} \equiv 1 \bmod \pi^{2p-1}.$$
We have shown that
$$(\frac{A}{\overline{A}})^p = 1+\lambda^{p-1+2m+1}b, \quad b \in K_p, \quad v_\pi(b)=0,$$

then

$$(1+\lambda^{p-1+2m+1}b)^{Q(\sigma)} \equiv 1 \bmod \pi^{2p-1}. \tag{23}$$

3. But $1+\lambda^{p-1+2m+1}b \equiv 1+p\lambda^{2m+1}b_1 \bmod \pi^{p-1+2m+2}$ with $b_1 \in \mathbb{Z}, \quad b_1 \not\equiv 0 \bmod p$. There exists a natural integer n not divisible by p such that

$$(1+p\lambda^{2m+1}b_1)^n \equiv 1+p\lambda^{2m+1} \bmod \pi^{p-1+2m+2}.$$

   Therefore

$$(1+p\lambda^{2m+1}b_1)^{nQ(\sigma)} \equiv (1+p\lambda^{2m+1})^{Q(\sigma)} \equiv 1 \bmod \pi^{p-1+2m+2}. \tag{24}$$

4. Show that the possibility of climbing up the step $\bmod \pi^{p-1+2m+2}$ implies that $\sigma - v^{2m+1}$ divides $Q(\sigma)$ in $\mathbf{F}_p[G_p]$: we have $(1+p\lambda^{2m+1})^{\sigma} = 1+p\sigma(\lambda^{2m+1}) = 1+p(\zeta^v-1)^{2m+1} = 1+p((\lambda+1)^v-1)^{2m+1} \equiv 1+pv^{2m+1}\lambda^{2m+1} \bmod \pi^{p-1+2m+2}$. In an other part $(1+p\lambda^{2m+1})^{v^{2m+1}} \equiv 1+pv^{2m+1}\lambda^{2m+1} \bmod \pi^{p-1+2m+2}$. Therefore

$$(1+p\lambda^{2m+1})^{\sigma-v^{2m+1}} \equiv 1 \bmod \pi^{p-1+2m+2}. \tag{25}$$

5. By euclidean division of $Q(\sigma)$ by $\sigma - v^{2m+1}$ in $\mathbf{F}_p[G_p]$, we get

$$Q(\sigma) = (\sigma - v^{2m+1})Q_1(\sigma) + R$$

   with $R \in \mathbf{F}_p$. From congruence (24) and (25) it follows that $(1+p\lambda^{2m+1})^R \equiv 1 \bmod \pi^{p-1+2m+2}$ and so that $1+pR\lambda^{2m+1} \equiv 1 \bmod \pi^{p-1+2m+2}$ and finally that $R=0$. Then in $\mathbf{F}_p$ we have $Q(\sigma) = (\sigma - v^{2m+1}) \times Q_1(\sigma)$ and so $Q(v^{2m+1}) \equiv 0 \bmod p$, or explicitly

$$Q(v^{2m+1}) = v^{(2m+1)(p-2)} \times \frac{v^{-(p-3)} - v^{-(p-2)}v}{p} + v^{(2m+1)(p-3)} \times \frac{v^{-(p-4)} - v^{-(p-3)}v}{p} + \dots$$
$$+ v^{2m+1} \times \frac{1 - v^{-1}v}{p} \equiv 0 \bmod p,$$

   which achieves the proof.

□

Remarks:

1. Observe that it is the π-adic theorem 2.15 connected to Kummer-Stickelberger which allows to obtain this result.

2. Observe that δ_i can also be written in the form $\delta_i = -[\frac{v^{-i}\times v}{p}]$ where $[x]$ is the integer part of x, similar form also known in the literature.
3. Observe that it is possible to get other polynomials of $\mathbb{Z}[G_p]$ annihilating the relative p-class group C_p^-: for instance from Kummer's formula on Jacobi cyclotomic functions we induce other polynomials $Q_d(\sigma)$ annihilating the relative p-class group C_p^- of K_p : If $1 \leq d \leq p-2$ define the set

$$I_d = \{i \mid 0 \leq i \leq p-2, \quad v^{(p-1)/2-i} + v^{(p-1)/2-i+ind_v(d)} > p\}$$

where $ind_v(d)$ is the minimal integer s such that $d \equiv v^s \bmod p$. Then the polynomials $Q_d(\sigma) = \sum_{i\in I_d} \sigma^i$ for $d = 1, \dots, p-2$ annihilate the p-class C_p of K_p, see for instance Ribenboim [5] relations (2.4) and (2.5) p. 119.
4. See also in a more general context Washington, [7] corollary 10.15 p. 198.
5. It is easy to verify the consistency of relation (22) with the table of irregular primes and Bernoulli numbers in Washington, [7] p. 410.

An immediate consequence is an explicit criterium for p to be a regular prime:

Corollary 3.2. *Let p be an odd prime. Let v be a primitive root $\bmod p$. If the congruence*

$$\sum_{i=1}^{p-2} X^{i-1} \times (\frac{v^{-(i-1)} - v^{-i} \times v}{p}) \equiv 0 \ mod\ p \tag{26}$$

has no solution X in $\mathbb{Z}$ with $X^{(p-1)/2} + 1 \equiv 0 \ mod\ p$ then the prime p is regular.

We give as another example a straightforward proof of following lemma on Bernoulli Numbers (compare elementary nature of this proof with proof hinted by Washington in exercise 5.9 p. 85 using Siegel-Brauer theorem).

Lemma 3.3. *If $2m+1 = \frac{p-1}{2}$ is odd then the Bernoulli Number $B_{(p+1)/2} \not\equiv 0 \ mod\ p$.*

Proof. From previous corollary it follows that if $B_{(p+1)/2} \equiv 0 \bmod p$ implies that $\sum_{i=1}^{p-2} v^{(2m+1)i} \times \delta^i \equiv 0 \bmod p$ where $2m+1 = \frac{p-1}{2}$ because $v^{(p-1)/2} \equiv -1 \bmod p$. Then suppose that

$$\sum_{i=1}^{p-2} (-1)^i \times (\frac{v^{-(i-1)} - v^{-i} \times v}{p}) \equiv 0 \bmod p,$$

and search for a contradiction: multiplying by p

$$\sum_{i=1}^{p-2} (-1)^i \times (v^{-(i-1)} - v^{-i} \times v) \equiv 0 \bmod p^2,$$

expanded to

$$(-1+v^{-1}-v^{-2}+\cdots-v^{-(p-3)})+(v^{-1}v-v^{-2}v+\cdots+v^{-(p-2)}v)\equiv 0 \bmod p^2$$

also

$$(-1+v^{-1}-v^{-2}+\cdots-v^{-(p-3)})+(v^{-1}-v^{-2}+\cdots+v^{-(p-2)})v\equiv 0 \bmod p^2.$$

Let us set $V=-1+v^{-1}-v^{-2}+\cdots-v^{-(p-3)}+v^{-(p-2)}$. Then we get $V-v^{-(p-2)}+v(V+1)\equiv 0 \bmod p^2$, and so $V(1+v)+v-v^{-(p-2)}\equiv 0 \bmod p^2$. But $v=v^{-(p-2)}$ and so $V\equiv 0 \bmod p^2$. But

$$\begin{aligned}
-V &= 1-v^{-1}+v^{-2}+\cdots+v^{-(p-3)}-v^{-(p-2)}=S_1-S_2\\
S_1 &= 1+v^{-2}+\cdots+v^{-(p-3)},\\
S_2 &= v^{-1}+v^{-3}+\cdots+v^{-(p-2)}.
\end{aligned}$$

v^{-1} is a primitive root mod p and so $S_1+S_2=\frac{p(p-1)}{2}$. Clearly $S_1\neq S_2$ because $\frac{p(p-1)}{2}$ is odd and so $-V=S_1-S_2\neq 0$ and $-V\equiv 0 \bmod p^2$ with $|-V|<\frac{p(p-1)}{2}$, contradiction which achieves the proof. □

4 Singular primary numbers and Stickelberger relation

In this section we give some π-adic properties of singular numbers A when they are primary. Recall that r, r^+, r^- are the ranks of the p-class groups C_p, C_p^-, C_p^+. Recall that $C_p=\oplus_{i=1}^r\Gamma_i$ where Γ_i are cyclic group of order p annihilated by $\sigma-\mu_i$ with $\mu_i\in\mathbf{F}_p^*$.

4.1 The case of C_p^-

A classical result on structure of p-class group is that the relative p-class group C_p^- is a direct sum $C_p^-=(\oplus_{i=1}^{r^+}\Gamma_i)\oplus(\oplus_{i=r^++1}^{r^-}\Gamma_i)$ where the subgroups $\Gamma_i,\quad i=1,\dots,r^+$ correspond to *singular primary* numbers A_i and where the subgroups $\Gamma_i,\quad i=r^++1,\dots,r^-$ corresponds to *singular not primary* numbers A_i. Let us fix one of these singular primary numbers A_i for $i=1,\dots,r^+$. Let $\mathbf{q}$ be a prime ideal of inertial degree f such that $A\mathbb{Z}[\zeta_p]=\mathbf{q}^p$.

Theorem 4.1. *Let $\mathbf{q}$ be a prime not principal ideal of $\mathbb{Z}[\zeta_p]$ of inertial degree f with $Cl(\mathbf{q})\in\Gamma\subset C_p^-$. Suppose that the prime number q above $\mathbf{q}$ verifies $p\parallel q^f-1$ and that A is a singular primary number with $A\mathbb{Z}[\zeta_p]=\mathbf{q}^p$. Then*

(27) $$A\not\equiv 1 \ mod\ \pi^{2p-1}.$$

Proof.

1. We start of the relation $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ proved in theorem 2.13. By conjugation we get $\overline{g(\mathbf{q})}^{p^2} = \pm \overline{A}^{P(\sigma)}$. Multiplying these two relations and observing that $g(\mathbf{q})\times\overline{g(\mathbf{q})} = q^f$ and $A\times\overline{A} = D^p$ with $D \in \mathbb{Z}[\zeta_p+\zeta_p^{-1}]$ we get $q^{fp^2} = D^{pP(\sigma)}$, so $q^{fp} = D^{P(\sigma)}$ because $q, D \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and, multiplying the exponent by $\sigma - v$, we get $q^{fp(\sigma-v)} = D^{P(\sigma)(\sigma-v)}$ so $q^{fp(1-v)} = D^{pQ(\sigma)}$ from lemma 2.10 p. 10 and thus

$$q^{f(1-v)} = D^{Q(\sigma)}. \tag{28}$$

2. Suppose that $\pi^{2p-1} \mid A - 1$. Then $\pi^{2p-1} \mid \overline{A} - 1$, so $\pi^{2p-1} \mid D^p - 1$ and so $\pi^p \mid D - 1$ and so $\pi^p \mid D^{Q(\sigma)} - 1$, thus $\pi^p \mid q^{f(1-v)} - 1$ and finally $\pi^p \mid q^f - 1$, contradiction with $\pi^{p-1} \parallel q^f - 1$.

□

In the following theorem we obtain a result of same nature which can be applied generally to a wider range of singular primary numbers A if we assume simultaneously the two hypotheses $q \equiv 1 \bmod p$ and $p^{(q-1)/p} \equiv 1 \bmod q$.

Theorem 4.2. *Let $\mathbf{q}$ be a prime not principal ideal of $\mathbb{Z}[\zeta_p]$ of inertial degree $f = 1$ with $Cl(\mathbf{q}) \in \Gamma \subset C_p$. Let A be a singular primary number with $A\mathbb{Z}[\zeta_p] = \mathbf{q}^p$. If $p^{(q-1)/p} \equiv 1$ mod q then there exists no natural integer a such that*

$$A \equiv a^p \ mod\ \pi^{2p}. \tag{29}$$

Proof. Suppose that $A \equiv a^p \bmod \pi^{2p}$ and search for a contradiction. We start of relation $g(\mathbf{q})^{p^2} = \pm A^{P(\sigma)}$ proved in theorem 2.13 p. 12. Therefore $g(\mathbf{q})^{p^2} \equiv \pm a^{pP(\sigma)} \bmod \pi^{2p}$, so

$$g(\mathbf{q})^{p^2} \equiv \pm a^{p(v^{-(p-2)}+\cdots+v^{-1}+1)} \bmod \pi^{2p},$$

so

$$g(\mathbf{q})^{p^2} \equiv \pm a^{p^2(p-1)/2} \bmod \pi^{2p}.$$

But $a^{p^2(p-1)/2} \equiv \pm 1 \bmod \pi^{2p}$. It should imply that $g(\mathbf{q})^{p^2} \equiv \pm 1 \bmod \pi^{2p}$, so that $g(\mathbf{q})^p \equiv \pm 1 \bmod \pi^{p+1}$ which contradicts lemma 2.8 p. 9. □

4.2 On principal prime ideals of K_p and Stickelberger relation

The Stickelberger relation and its consequences on prime ideals $\mathbf{q}$ of $\mathbb{Z}[\zeta_p]$ is meaningful even if $\mathbf{q}$ is a principal ideal.

Theorem 4.3. *Let $q_1 \in \mathbb{Z}[\zeta_p]$ with $q_1 \equiv a \mod \pi^{p+1}$ where $a \in \mathbb{Z}$, $\quad a \not\equiv 0 \mod p$. If $q = N_{K_p/\mathbb{Q}}(q_1)$ is a prime number then $p^{(q-1)/p} \equiv 1 \mod q$.*

Proof. From Stickelberger relation $g(q_1\mathbb{Z}[\zeta_p])^p\mathbb{Z}[\zeta_p] = q_1^{P(\sigma)}\mathbb{Z}[\zeta_p]$ and so there exists $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ such that $g(q_1\mathbb{Z}[\zeta_p])^p = q_1^{P(\sigma)} \times \varepsilon$ and so

$$(\frac{g(q_1\mathbb{Z}[\zeta_p])}{\overline{g(q_1\mathbb{Z}[\zeta_p]}})^p = (\frac{q_1}{\overline{q_1}})^{P(\sigma)}.$$

From hypothesis $\frac{q_1}{\overline{q_1}} \equiv 1 \mod \pi^{p+1}$ and so $(\frac{g(q_1\mathbb{Z}[\zeta_p]}{\overline{g(q_1\mathbb{Z}[\zeta_p]}})^p \equiv 1 \mod \pi^{p+1}$. From lemma 2.8 p. 9 it follows that $p^{(q-1)/p} \equiv 1 \mod q$. □

5 Stickelberger's relation for prime ideals q of inertial degree $f > 1$.

Recall that the Stickelberger's relation is $g(\mathbf{q})^p = \mathbf{q}^S$ where $S = \sum_{i=0}^{p-2} \sigma^i v^{-i} \in \mathbb{Z}[G_p]$. We apply Stickelberger's relation with the same method to prime ideals $\mathbf{q}$ of inertial degree $f > 1$. Observe, from lemma 2.2 p. 5, that $f > 1$ implies $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$.

A definition: we say that the prime ideal $\mathbf{c}$ of a number field M is p-principal if the component of the class group $< Cl(\mathbf{c}) >$ in p-class group D_p of M is trivial.

Lemma 5.1. *Let p be an odd prime. Let v be a primitive root $\mod p$. Let q be an odd prime with $q \neq p$. Let f be the smallest integer such that $q^f \equiv 1 \mod p$ and let $m = \frac{p-1}{f}$. Let $\mathbf{q}$ be an prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. If $f > 1$ then $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$ and $g(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_2}$ where*

$$S_2 = \sum_{i=0}^{m-1} (\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times \sigma^i \in \mathbb{Z}[G_p]. \tag{30}$$

Proof.

1. Let $p = fm+1$. Then $N_{K_p/\mathbb{Q}}(\mathbf{q}) = q^f$ and $\mathbf{q} = \mathbf{q}^{\sigma^m} = \dots = \mathbf{q}^{\sigma^{(f-1)m}}$. The sum S defined in lemma 2.5 p.7 can be written

$$S = \sum_{i=0}^{m-1} \sum_{j=0}^{f-1} \sigma^{i+jm} v^{-(i+jm)}.$$

2. From Stickelberger's relation seen in theorem 2.1 p. 5, then $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^S$. Observe that, from hypothesis, $\mathbf{q} = \mathbf{q}^{\sigma^m} = \cdots = \mathbf{q}^{\sigma^{(f-1)m}}$ so Stickelberger's relation implies that $g(\mathbf{q})^p\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_1}$ with

$$S_1 = \sum_{i=0}^{m-1}\sum_{j=0}^{f-1}\sigma^i v^{-(i+jm)} = p \times \sum_{i=0}^{m-1}(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times \sigma^i,$$

where $(\sum_{i=0}^{f-1} v^{-(i+jm)})/p \in \mathbb{Z}$ because $v^{-m} - 1 \not\equiv 0 \bmod p$.

3. Let $S_2 = \frac{S_1}{p}$. From lemma 2.2 p. 5 we know that $f > 1$ implies that $g(\mathbf{q}) \in \mathbb{Z}[\zeta_p]$. Therefore

$$g(\mathbf{q})\mathbb{Z}[\zeta_p] = \mathbf{q}^{S_2}, \quad g(\mathbf{q}) \in \mathbb{Z}[\zeta_p].$$

□

It is possible to derive some explicit congruences in $\mathbb{Z}$ from this result.

Lemma 5.2. *Let p be an odd prime. Let v be a primitive root $\bmod p$. Let q be an odd prime with $q \neq p$. Let f be the smallest integer such that $q^f \equiv 1 \bmod p$ and let $m = \frac{p-1}{f}$. Let $\mathbf{q}$ be an prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q.*

1. *If $f > 1$ and if $\mathbf{q}$ is not p-principal ideal there exists a natural integer l, $1 \leq l < m$ such that*

$$\sum_{i=0}^{m-1}(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times v^{lfi} \equiv 0 \ mod\ p, \tag{31}$$

2. *If for all natural integers l such that $1 \leq l < m$*

$$\sum_{i=0}^{m-1}(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}) \times v^{lfi} \not\equiv 0 \ mod\ p, \tag{32}$$

   then $\mathbf{q}$ is p-principal

Proof.

1. Suppose that $\mathbf{q}$ is not p-principal. Observe at first that congruence (31) with $l = m$ should imply that $\sum_{i=0}^{m-1}(\sum_{j=0}^{f-1} v^{-(i+jm)})/p) \equiv 0 \bmod p$ or $\sum_{i=0}^{m-1}\sum_{j=0}^{f-1} v^{-(i+jm)} \equiv 0 \bmod p^2$ which is not possible because $v^{-(i+jm)} = v^{-(i'+j'm)}$ implies that $j = j'$ and $i = i'$ and so that $\sum_{i=0}^{m-1}\sum_{j=0}^{f-1} v^{-(i+jm)} = \frac{p(p-1)}{2}$.

2. The polynomial S_2 of lemma 5.1 annihilates the not p-principal ideal $\mathbf{q}$ in $\mathbf{F}_p[G_p]$ only if there exists $\sigma - v^n$ dividing S_2 in $\mathbf{F}_p[G_p]$. From $\mathbf{q}^{\sigma^m - 1} = 1$ it follows also that $\sigma - v^n \mid \sigma^m - 1$. But $\sigma - v^n \mid \sigma^m - v^{nm}$ and so $\sigma - v^n \mid v^{nm} - 1$, thus $nm \equiv 0 \bmod p-1$, so $n \equiv 0 \bmod f$ and $n = lf$. Therefore if $\mathbf{q}$ is not p-principal there exists a natural integer $l,\ 1 \leq l < m$ such that

$$\sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}\right) \times v^{lfi} \equiv 0 \bmod p, \tag{33}$$

3. The relation (32) is an imediate consequence of previous part of the proof.

□

As an example we deal with the case $f = \frac{p-1}{2}$.

Corollary 5.3. *If $p \equiv 3$ mod 4 and if $f = \frac{p-1}{2}$ then $\mathbf{q}$ is p-principal.*

Proof. We have $f = \frac{p-1}{2}$, $m = 2$ and $l = 1$. Then

$$\Sigma = \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v^{-(i+jm)}}{p}\right) \times v^{lfi} = \frac{\sum_{j=0}^{(p-3)/2} v^{-2j}}{p} - \frac{\sum_{j=0}^{(p-3)/2} v^{-(1+2j)}}{p}. \tag{34}$$

$\Sigma \equiv 0 \bmod p$ should imply that $\sum_{j=0}^{(p-3)/2} v^{-2j} - \sum_{j=0}^{(p-3)/2} v^{-(1+2j)} \equiv 0 \bmod p^2$. But $\sum_{j=0}^{(p-3)/2} v^{-2j} + \sum_{j=0}^{(p-3)/2} v^{-(1+2j)} = \frac{p(p-1)}{2}$ is odd, which achieves the proof. □

References

[1] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.

[2] H. Koch, *Algebraic Number Theory*, Springer, 1997.

[3] R.A. Mollin, *Algebraic Number Theory*, Chapman and Hall/CRC, 1999.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Numbers*, Springer-verlag, 1990.

[5] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[6] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[7] L.C. Washington, *Introduction to cyclotomic fields, second edition*, Springer, 1997.